



面向 MANET 报文丢弃攻击的模糊入侵检测系统

陆婷婷¹, 韩旭²

(1. 江苏食品药品职业技术学院, 江苏 淮安 223003;

2. 河南牧业经济学院信息与电子工程学院, 河南 郑州 450044)

摘要: 为了检测 MANET 报文丢弃攻击行为, 提出一种异常模糊入侵检测系统(FIADS)。FIADS 基于 Sugeno 型模糊推理, 通过分布式方式检测每个节点可能遭受的攻击行为, 并通过移除所有可能实施攻击的恶意节点提高 MANET 频谱资源。最后, 构建模糊规则库仿真分析了 FIADS, 并和传统 IDES 进行了性能比较。仿真结果证明, 相比 IDES, FIADS 能够有效检测报文丢弃攻击, 具有更高的识别效率。

关键词: 移动无线自组织网络; 报文丢弃攻击; 模糊入侵; 入侵检测系统; Sugeno 型模糊推理系统

中图分类号: TP.393.03

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016263

Fuzzy intrusion detection system for MANET packet dropping attack

LU Tingting¹, HAN Xu²

1. Jiangsu Food and Pharmaceutical Science College, Huai'an 223003, China

2. School of Information and Electronic Engineering, Henan University of Animal
Husbandry and Economy, Zhengzhou 450044, China

Abstract: For further detecting the packet dropping attack action, a fuzzy intrusion abnormality-based detection system (FIADS) was proposed. Based on Sugeno-type fuzzy inference system, FIADS detected the attack actions of each node by a distributed manner, and then moved these malicious nodes out of MANET to improve the frequency spectrum resource of MANET. Finally, fuzzy rules base was made to analyze FIADS, and comparison between FIADS and the traditional IDES was made. The simulation results show that, compared with IDES, FIADS can effectively detect the packet dropping attack action, and owns a higher detection efficiency.

Key words: wireless Ad Hoc network, packet dropping attack, fuzzy intrusion, intrusion detection system, Sugeno-type fuzzy inference system

1 引言

移动 Ad Hoc 网络(mobile Ad Hoc network, MANET)使用无线链路传输信息, 由于无线链路具有开放和拓扑动态变化等特性^[1], 更易遭受恶意攻击, 目前针对网络层的

攻击主要有黑洞攻击^[2]、虫洞攻击^[3]、灰洞攻击^[4]和报文丢弃攻击^[5]等。黑洞攻击是指网络节点被恶意攻陷后, 丢弃所有收到的分组, 就像“黑洞”一样对其他节点没有任何响应; 虫洞攻击是指多个被攻击节点以协作方式攻击路由资源进而破坏拓扑结构; 灰洞攻击则是一种特殊

的黑洞攻击,通过选择性转发报文实现对网络正常通信的干扰,不同于黑洞攻击行为,恶意节点在实施报文丢弃攻击行为中,依然和其他节点进行正常通信,具有更强的隐蔽性。

报文丢弃攻击也是 MANET 遭受的一种常见攻击方式,通常是在 MANET 某节点被俘叛变后,在报文传输过程中进行实施^[6]。报文丢弃攻击的恶意节点在丢弃报文时,通过阻止其他节点转发丢弃的报文,具有更严重的攻击效果。因此,本文主要研究报文丢弃攻击行为检测。目前使用认证和加密消除 MANET 安全威胁并不能抵抗来自掌握密钥的内部叛变节点的攻击行为。而入侵检测系统(intrusion detection system,IDS)设计则成为保护 MANET 安全性的关键技术,是网络安全性的第二防火墙。

目前主流入侵检测系统分为滥用检测、异常检测两类^[7]。滥用检测通过预定义传统攻击类型的行为特征实现攻击检测,具有较低的误判率,但是检测不出新攻击类型,典型算法有 IDIOT^[8]和 STAT^[9]。异常检测是基于正常系统行为,检测异常行为判断是否受到攻击,能够检测新类型和未知攻击,但由于系统状态实时变化,定义系统行为难度大,并且系统误判率较高,典型算法有入侵检测专家系统(intrusion detection expert system,IDES)^[10],而目前大多数异常检测系统均是借鉴 IDES 思想或者以 IDES 为原型改进而成,如基于遗传神经网络的入侵检测系统^[11]、基于多层前向神经网络的入侵检测系统^[12]等。此外,由于入侵活动具有模糊特征,通过将入侵检测转化为对多模糊证据的综合判决可以有效判断入侵行为检测的不确定程度,目前针对 MANET 报文丢弃攻击的模糊入侵检测系统研究甚少。

本文提出了一种异常模糊入侵检测系统(fuzzy intrusion abnormality-based detection system,FIADS)就是基于上述考虑,使用了 Sugeno 类型模糊推理逻辑方法检测来自恶意节点的报文丢弃攻击。FIADS 以分布式方式检测每个节点遭受的数据丢弃攻击,从而删除 MANET 中所有可能实施报文丢弃攻击的恶意节点。最后,将本文所提方案与经典模型 IDES 仿真对照,比较分析了网络的分组转发率、分组丢弃率和节点真实度水平等性能指标,验证了 FIADS 的有效性。

2 模糊逻辑技术

模糊逻辑技术能够有效解决由人为原因造成的不精确和不确定问题,本节主要介绍 FIADS 中的模糊逻辑设

计。使用基于模糊逻辑的 if-then-else 规则定义 MANET 所有,以识别所有可能的攻击和入侵行为。模糊逻辑的基本功能如图 1 所示。

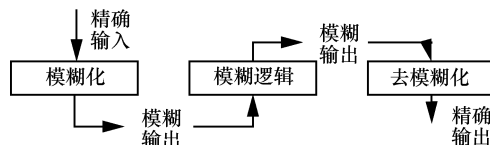


图 1 模糊逻辑基本功能

模糊推理系统类型主要有 Mamdani 类型和 Sugeno 类型^[13],本方案选择基于双输入单输出的一阶 Sugeno 模糊推理系统实现 FIADS 决策,如图 2 所示。

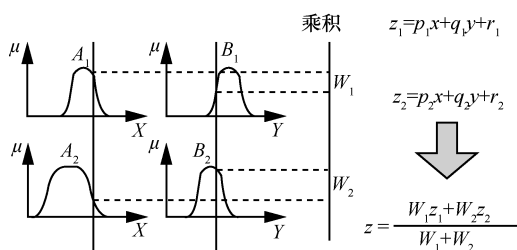


图 2 Sugeno 模糊推理系统模型

如图 2 所示,以具有两条逻辑规则的某 Sugeno 模型为例,其规则分别为:如果 x 是 A_1 且 y 是 B_1 ,则有 $z_1 = p_1x + q_1y + r_1$;如果 x 是 A_2 且 y 是 B_2 ,则有 $z_2 = p_2x + q_2y + r_2$ 。 A_1, A_2 和 B_1, B_2 分别是模糊集 A 和 B 的输入隶属度函数, z_1 和 z_2 分别为子系数输出。 p_1, q_1, r_1, p_2, q_2 和 r_2 均为常数,由系统大量输入输出数据经过辨识获取。 W_1 和 W_2 分别为 z_1 和 z_2 的加权系数,分别有 $W_1 = A_1(x)B_1(y), W_2 = A_2(x)B_2(y)$, z 为 Sugeno 模糊系统输出。此外,图 2 横轴为 X, Y ,表示隶属度函数输入值, μ 为纵轴,表示隶属度函数输出值。

3 FIADS 系统

图 3 为 FIADS 模型。据图 3 可知,FIADS 由模糊参数提取模块、模糊推理模块、模糊决策模块和响应模块组成。FIADS 使用模糊参数提取模块从网络业务模块中提取必需参数,将其输入 Sugeno 模糊推理系统进行分析。通过使用各种模糊规则和隶属度函数对这些参数计算,

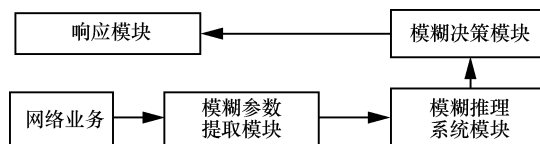


图 3 FIADS 模型



得到模糊推理模块中节点真实度水平,将其和相应门限值作比较。如果真实度水平小于门限值,则认为该节点行为恶意,进而从响应模块中激活标识该特殊节点 IP 地址的警告。

3.1 模糊参数提取模块

该模块通过侦听周围直接邻居节点的业务,进而提取输入模糊推理系统中的主要参数,网络节点创建邻居信息表,存储每个邻居节点并保存这些参数。每个节点都可以侦听其直接邻居节点业务并收集用于模拟推理系统的输入参数。邻居信息表主要存储邻居节点的数据分组转发率、平均数据分组丢弃率和真实性水平等参数。

数据分组转发率是通过侦听周围直接邻居节点所有业务,获得邻居节点上直接收到的数据分组数目,再通过此邻居节点转发的数据分组计算得到。

平均数据分组丢弃率是通过计算每个邻居节点的接收数据分组数目和转发数据分组数目。由于本系统中,MANET 使用的是 AODV 路由协议^[14],接收的分组数目必须转发给路由下一跳节点,故两者数目之差不会太大。因此,如果是恶意节点,则两者数目之差必然会很大。本系统计算了邻居信息表中所有路由的中间节点的平均分组丢弃率。

使用真实性水平作为 MANET 中任意一个节点可能存在的恶意行为的评估指标,真实性水平值区间为[0,10],真实性水平值越低,节点受到恶意攻击的可能性越大。每个节点都将计算其直接邻居节点的真实性水平,并将其存入其邻居节点信息表中。以网络任一节点 C 为例,给出节点 C 的模糊参数提取算法流程,如算法 1 所示。

算法 1

function Y=Parameter_Extract()

(1) 初始化 Neighbor_list {Address; num_pkt_rcvd; num_pkt_sent; rate_pkt_transfer; rate_pkt_discard; real_level}

(2) If (Status(C)==Receiving)//判断节点接收状态

(3) {

(4) If(有分组到达)

(5) {

(6) Address=dest_addr;

(7) Neighbor_list(dest_addr)->num_pkt_rcvd++;

(8) If(src_addr 是邻居节点)

(9) {

(10) Neighbor_list(src_addr)->num_pkt_sent++;

(11) }

(12) }

(13) }

(14) For (i=1;i<=Size(Neighbor_list);i++)

(15) {

(16) Neighbor_list(i)->rate_pkt_transfer=Neighbor_list(i)

->num_pkt_sent/num_pkt_rcvd;

(17) Neighbor_list(i)->rate_pkt_discard=Neighbor_list(i)

->(num_pkt_rcvd-num_pkt_sent)/num_pkt_rcvd;

(18) 据表 1 模糊规则计算邻居节点 i 真实性水平;

(19) Neighbor_list(i)->real_level=Fusion_Computing();

(20) }

3.2 模糊推理模块

FIADS 使用 Sugeno 模糊推理系统分析 MANET 中节点的系统行为。FIADS 中,使用来自网络业务的报文转发率和报文丢弃率作为模糊推理模块输入参数,将节点真实性水平作为此模块输出。FIADS 使用节点真实性衡量节点行为,表示节点为正常节点或恶意节点,输入参数使用表 1 所示的模糊规则评估输出结果。

表 1 FIADS 模糊规则评估输出结果

报文转发率	报文丢弃率	真实性水平
高	低	高
高	中	高
高	高	低
中	低	中
中	中	中
中	高	低
低	低	低
低	中	低
低	高	低

为得到最优性能,用于输入和输出参数的隶属度函数如图 4 所示。在模糊推理系统中,规则库中的第一条规则解释如下:如果报文转发率高并且平均报文丢弃率低,则真实性水平高。计算每个节点邻居信息表上所有邻居节点的真实性水平,表示其参数隶属性函数。真实性水平在 0~10 内。因此,低真实性水平表示节点恶意可能;反之,高真实性水平则表示节点正常可能性大。0 表示节点行为完全恶意,10 表示节点行为完全正常。算法 2 是 FIADS 模糊推理模块的算法流程。

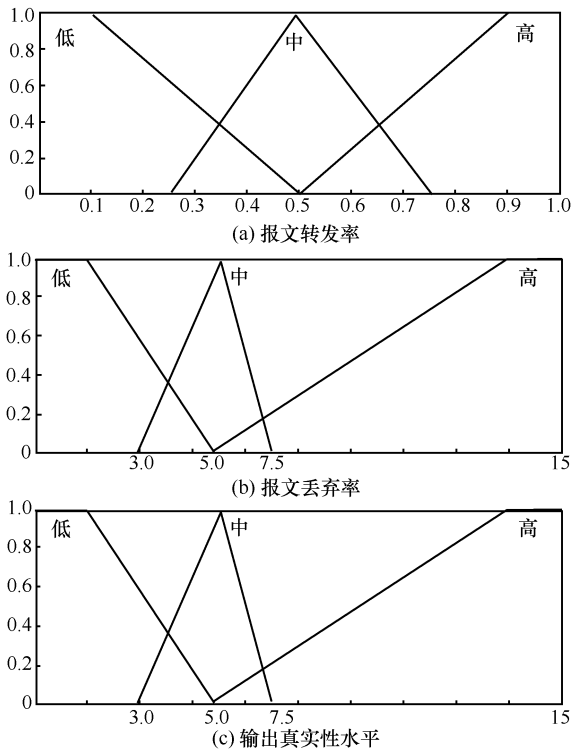


图 4 输入和输出参数的隶属度函数

算法 2

function Y=Fusion_Computing()

(1) 初始化:数据结构

Temp {address; rate_pkt_transfer; rate_pkt_discard; }

Result

{address;pkt_transfer_level;pkt_discard_level;real_level};

(2) For (i=1;i<Size(Neighbor_list);i++)

(3) {

(4) Temp->address=Neighbor_list(i)->address;

(5) Temp->rate_pkt_transfer=Neighbor_list(i)->rate_pkt_transfer;

(6) Temp->rate_pkt_discard=Neighbor_list(i)->rate_pkt_discard;

(7) 根据图 5(a)、图 5(b)的隶属度函数分别求解出 Result(i)->pkt_transfer_level 和 pkt_discard_level;

(8) 再根据表 1 的模糊规则求出

(9) Result(i)->real_level;

}

3.3 模糊决策模块

此模块中,真实性水平门限被设置用于和真实性水平计算值进行比较,用以分析 MANET 中的节点行为。本文

中设置门限值为 5.5。比较过程中,如果真实性水平>5.5,则表示节点为正常节点,否则为恶意节点。

3.4 复杂性分析

不同于传统 IDES 使用专家推理和决策机制,FIADS 使用 Sugeno 类型模糊推理和模糊决策机制,针对通信流量开销方面,FIADS 提取参数的类型、方法与 IDES 相同,均是通过侦听分组实现,故通信流量开销相同;而针对计算量,虽然 FIADS 使用隶属度函数增加了一定计算量,但 IDES 因为使用专家知识库推理分析,占用了更多的存储空间用于存储专家经验知识。综上所述,FIADS 和 IDES 两者复杂性各有优劣,通信开销流量相同,FIADS 消耗存储空间较小,IDES 计算量较小,但相比 IFADS 在识别精确度方面具有的性能优势,两者复杂性差异可以近似忽略。

4 仿真结果分析

4.1 仿真环境设置

首先使用 QualNet 仿真器 6.1^[15,16]仿真模拟遭受恶意节点进行报文丢弃攻击的 MANET,仿真中,网络节点数目为 30,路由协议使用 AODV,MAC 协议为 IEEE 802.11^[17],节点使用随机路点移动模型^[18],移动速度从 1 m/s 到 25 m/s,业务分布模型使用 CBR 业务。场景中,负责丢弃报文的恶意节点数目有 4、10 和 20。从 QualNet 仿真器中提取到相关仿真数据结果后,再使用 MATLAB 软件模糊工具箱处理。最后,比较了 FIADS 和传统 IDES 的识别率性能,IDES 相关参数设置见参考文献[10]。

4.2 性能分析

首先,分析在不同节点移动速度条件下 FIADS 和 IDES 关于识别率和误判率的仿真结果,如图 5 所示。据图 5 可

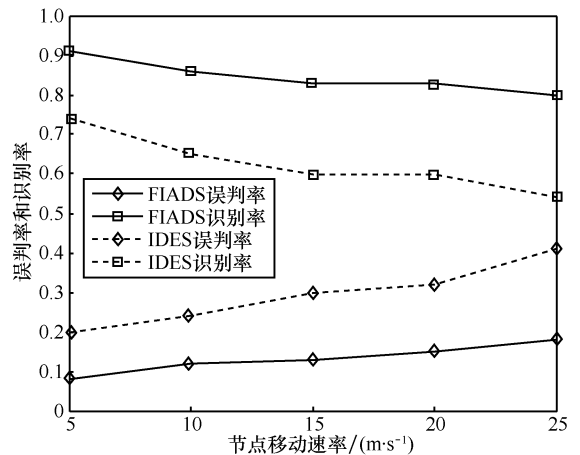


图 5 FIADS 和 IDES 检测系统性能比较



知,相比 IDES,FIADS 具有更高的报文丢弃攻击识别率和较低的误判率,这是因为 FIADS 使用模糊逻辑判断所致,而传统 IDES 则使用了简单 0 或 1 的判决机制,误判率很高。不同移动速率级别条件下 FIADS 识别结果见表 2。

表 2 不同移动速率级别条件下 FIADS 系统识别结果

节点移动速度	识别率	误判率
低	97%	0.8%
中	92.5%	1.2%
高	89%	1.75%

其次,分析了 FIADS 检测性能受节点真实性水平门限值的影响,仿真结果如图 6 所示。据图 6 可知,如果门限值较小,误判率较高,正常节点被误判为恶意节点;反之,如果门限值较大,误判率较低,但识别性能较差,这是因为恶意节点被当作正常节点。

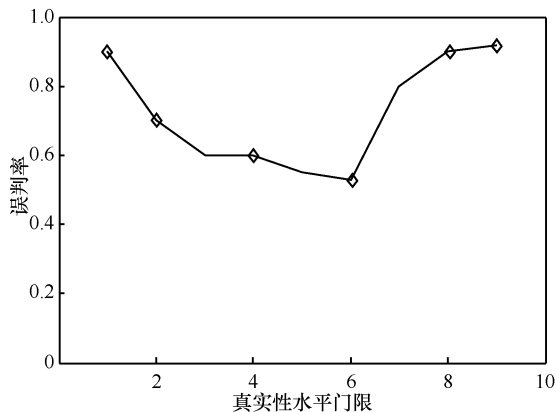


图 6 FIADS 检测性能及节点真实性水平门限

5 结束语

本文基于模糊逻辑规则,设计了一种基于异常检测的 FIADS 报文丢弃攻击检测系统用于检测 MANET 中恶意节点的报文丢弃攻击行为,该系统使用 Sugeno 类型模糊推理系统作为 FIADS 核心模糊推理模块。最后使用 QualNet 软件和 MATLAB 模糊逻辑工具箱分别仿真了 MANET 和 FIADS,并和传统异常检测 IDES 进行识别性能比较。仿真结果证明,FIADS 具有可靠的恶意节点检测性能,相比传统检测系统具有更高的检测识别性能和较低的误判率。

参考文献:

[1] 周欣欣,余镇危. 基于情景感知的移动 Ad Hoc 网络自适应路由协议[J]. 计算机工程与设计, 2014, 35(11): 3799-3904.

ZHOU X X, YU Z W. Adaptive routing protocol based on context-aware for mobile Ad Hoc networks [J]. Computer Engineering and Design, 2014, 35(11): 3799-3904.

[2] 卜飞飞, 邹春学. 一种针对 AODV 协议黑洞攻击的检测策略[J]. 计算机应用与软件, 2015, 32(5): 273-277.

BU F F, WU C X. A detection strategy for black hole attack based on AODV[J]. Computer Applications and Software, 2015, 32(5): 273-277.

[3] 葛洁莉, 刘渊. 一种抵御虫洞攻击的 WSN 定位算法[J]. 计算机与现代化, 2015(8): 61-66.

GE J L, LIU Y. A WSN location algorithm against wormhole attacks[J]. Computer and Modernization, 2015(8): 61-66.

[4] 温聪源, 徐守萍. 基于改进动态源路由协议的 MANET 灰洞攻击检测和缓解研究 [J]. 科学技术与工程, 2014, 14(29): 54-60.

WEN C Y, XU S P. The research of detecting and mitigating gray hole attacks in MANET based on modified dynamic source routing protocol [J]. Science Technology and Engineering, 2014, 14(29): 54-60.

[5] 靳倩慧, 姚国祥, 李佩. MANET 分簇 IDS 报文丢弃攻击全局感知方案[J]. 微型机与应用, 2011, 30(17): 49-53.

JIN Q H, YAO G X, LI P. A scheme of globally detecting packet dropping attacks for clustering IDS in MANET [J]. Microcomputer and Application, 2011, 30(17): 49-53.

[6] 钟飞, 钟毓宁. Mamdani 与 Sugeno 型模糊推理的应用研究[J]. 湖北工业大学学报, 2005, 20(2): 27-30.

ZHONG F, ZHONG Y N. The application research of Mamdani and Sugeno style fuzzy inference[J]. Journal of Hubei University of Technology, 2005, 20(2): 27-30.

[7] SAMEEKSHA J, AMIT J. Survey on intrusion detection system for wireless Ad Hoc network [J]. International Journal of Computer Applications, 2015, 120(4): 14-19.

[8] LEANDROS A M. A novel distributed intrusion detection system for vehicular ad hoc networks [J]. International Journal of Advanced Computer Science and Applications, 2015, 6(4): 101-106.

[9] 陈丹伟, 黄秀丽, 任勋益. 基于人工神经网络入侵检测模型的探讨[J]. 计算机技术与发展, 2009, 19(12): 143-145.

CHEN D W, HUANG X L, REN X Y. An approach to IDS model based on artificial neuron networks [J]. Computer Technology and Development, 2009, 19(12): 143-145.

[10] 刘道群, 孙庆和. 基于遗传神经网络的入侵检测模型 [J]. 激光杂志, 2005, 26(6): 73-75.

LIU D Q, SUN Q H. Intrusion detection method based on genetic algorithm and neural network [J]. Laser Journal, 2005, 26(6): 73-75.

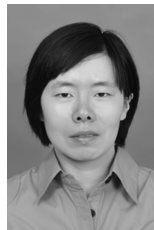
[11] 马海峰, 孙名松. 基于多层前向神经网络入侵检测系统的研究[J]. 哈尔滨理工大学学报, 2004, 9(2): 52-55.

- MA H F, SUN M S. Study of intrusion detection system based on multiplayer forward neural network [J]. Journal of Harbin University of Science and Technology, 2004, 9(2): 52-55.
- [12] 李向远, 张章, 李杨. 基于 QualNet 的一种分布式空中骨干网的研究与设计[J]. 舰船电子工程, 2015, 35(5): 43-46.
- LI X Y, ZHANG Z, LI Y. Research and design of distributed air backbone network based on QualNet [J]. Ship Electronic Engineering, 2015, 35(5): 43-46.
- [13] 王桐. 一种新的无线网络信号干扰累加捕获模型[J]. 南京师范大学学报(工程技术版), 2015, 15(2): 73-76.
- WANG T. A new capture model based on cumulative signal interference for wireless ad hoc networks [J]. Journal of Nanjing Normal University (Engineering and Technology Edition), 2015, 15(2): 73-76.
- [14] 石柯, 陈洪生, 张仁同. 一种基于支持向量回归的 802.11 无线室内定位方法[J]. 软件学报, 2014, 25(11): 2636-2651.
- SHI K, CHEN H S, ZHANG R T. Indoor location method based on support vector regression in 802.11 wireless environments[J]. Journal of Software, 2014, 25(11): 2636-2651.
- [15] 李晖. 移动容迟网络中基于改进随机路点模型的移动连接路由[J]. 吉林大学学报(工学版), 2011, 41(S1): 297-303.
- LI H. Mobile connection routing under modified random waypoint models in delay tolerant mobile networks [J]. Journal of Jilin University (Engineering Edition), 2011, 41 (S1): 297-303.
- [16] SIMAREMATE H, SYARIF A, ABOUAISSA A. Energy consumption analysis of modified AODV routing protocol under random waypoint and reference point group mobility models[C]// International Conference on Advanced Computer Science and Information Systems, Dec 1-2, 2012, Jakarta, Indonesia. New Jersey: IEEE Press, 2012.
- [17] 刘侠, 肖英杰, 吴华锋. 联合无线资源管理技术的改进型垂直切换算法[J]. 电子技术应用, 2014, 40(2): 97-100.
- LIU X, XIAO Y J, WU H F. An improved vertical handoff algorithm of joint radio resource management [J]. Application of Electronic Technique, 2014, 40(2): 97-100.
- [18] 彭蜜. 像素方向分布不一致性的图像模糊取证方法[J]. 电子技术应用, 2014, 40(4): 63-69.
- PENG M. Blurring detection in image forensics based on pixels direction inconsistency [J]. Application of Electronic Technique, 2014, 40(4): 63-69.

[作者简介]



陆婷婷(1981-),女,江苏食品药品职业技术学院讲师,主要研究方向为计算机网络与图形图像。



韩旭(1980-),女,现就职于河南牧业经济学院信息与电子工程学院,主要研究方向为通信网络。